Embodiment	Key Type	Identity Element	TA Element	Session Element	General Form
First	Encryption “Enc”	Q_{IDi} Public	R_{TAi} Public	r Private	$\prod t(R_{\mathrm{TA}i}, rQ_{\mathrm{ID}i})$
	Decryption “Dec”	S_{i} Private Q_{IDi}in S_{i}	s_i in S_{i}	U Public	$t(U, \sum b_i S_i)$
Second	Encryption “gID”	Q_{IDi} Public	P_{pubi} Public	σ Private	$\Pi\hat{e}(Q_{\mathrm{IDi}}, P_{pubi})$
	Decryption “x”	d_{IDi} Private Q_{IDi}in d_{IDi}	s_i in d_{IDi}	U Public	$\hat{e}(\Sigma\, d_{\mathrm{IDi}}, U)$
Third	Signature (compound)	d_{IDi} Private	P_{pubi} Public	z Private	$h\,\Sigma\, d_{\mathrm{IDi}} + z\,\Sigma P_{pubi}$
	Verification (compound)	Q_{IDi} Public	P_{pubi}, U Public	U Public	$\Pi\hat{e}(P_{pubi}, hQ_{\mathrm{IDi}} + U)$
Fourth	Signature “e”	d_{IDi} Private Q_{IDi}in d_{IDi}	s_i in d_{IDi}	k Private	$\hat{e}(\Sigma\, d_{\mathrm{IDi}}, P)$
	Verification ”’e’”	Q_{IDi} Public	P_{pubi} Public	h, S Public	$\Pi\hat{e}(Q_{\mathrm{IDi}}, P_{pubi})$

Figure 3